AMENDMENTS

In the Claims

The following is a marked-up version of the claims with the language that is underlined ("___") being added and the language that contains strikethrough ("—") being deleted:

1. (Currently Amended) A method for securely communicating information, said method comprising:

communicating an address to a first network device via the Internet such that the first network device provides information corresponding to the address for use by a second network device;

receiving encrypted information from the first network device via the Internet;

enabling the encrypted information to be posted at the address; and

enabling the second network device to access the address and retrieve the encrypted information posted at the address;

wherein the address provided to the first network device is a first Uniform Resource Locator (URL) configured for a one-time use; and

wherein the second network device retrieves the encrypted information using a second URL, the second URL being configured for a one-time use.

2. (Canceled)

3. (Currently Amended) The method of claim [[2]] 1, wherein a first firewall is communicatively coupled between the first network device and the Internet.

4. (Canceled)

5. (Original) The method of claim 1, wherein the encrypted information is provided from the first network device to the second network device without either of the first and second network devices being identified to the other.

6. (Currently Amended) The method of claim 1, wherein the address [[is]] provided to the second network device is provided via a mobile appliance, the mobile appliance communicating with the first and second network devices via wireless communication links.

7. (Original) The method of claim 1, wherein a decryption key is provided to the second network device via a secure communication protocol, the decryption key being configured to enable decryption of the encrypted information.

8. (Original) The method of claim 7, wherein the secure communication protocol uses the Bluetooth specification.

9. (Original) The method of claim 7, wherein the decryption key is provided to the second network device via a mobile appliance, the mobile appliance communicating with the first and second network devices via wireless communication links.

10. (Original) The method of claim 9, wherein the decryption key is generated by the first network device; and

wherein the mobile appliance receives the decryption key from the first network device.

11. (Original) The method of claim 1, wherein the second network device is a printing device configured to receive the encrypted information, decrypt the information, and print the information.

12. (Currently Amended) A system for enabling secure communication of information between a first network device and a second network device via the Internet, said system comprising:

a secure tunnel system communicating with the Internet;

the secure tunnel system being configured to:

provide address information to a first network device via the Internet;

receive encrypted information from the first network device via the Internet;

post the encrypted information ~~at an address~~ using a first one-time use URL associated with the address information; and

enable a second network device to access and retrieve the encrypted information ~~from the address~~ via the Internet using a second one-time use URL while the encrypted information is posted.

13. (Currently Amended) The system of claim 12, wherein the secure tunnel system is configured to provide the first one-time use URL and the seocnd one-time use URL ~~prevent the encrypted information from being retrieved again after the encrypted information has been retrieved by the second network device~~.

14. – 15. (Canceled)

16. (Currently Amended) A method for securely communicating information, said method comprising:

providing a first network device;

receiving, at the first network device, an address via the Internet;

~~providing a decryption key and the address to a mobile appliance via a secure communication link; and~~

~~providing encrypted information to the address via the Internet, such that a second network device is enabled to access and retrieve the encrypted information from the address via the Internet while the encrypted information is posted and decrypt the information using the decryption key provided from the mobile appliance~~

receiving an input from a user, the input corresponding to the user's intent to have information communicated to a second network device;

in response to the user input, establishing communication with a third network device via the Internet, the third network device being configured to provide the first network device with a first Uniform Resource Locator (URL) for use by the first network device and a second URL for use by the second network device, the first URL being configured for a one-time use such that the first network device can post encrypted information at the address using the first URL, the second URL being configured for a one-time use such that the second network device can retrieve the encrypted information from the address using the first URL; and

receiving the first and second URL's from the third network device.

17. (Canceled)

18. (Original) The method of claim 16, further comprising:

generating a decryption key for decrypting the encrypted information.

19. (Currently Amended) A system for enabling secure communication of information between a first network device and a second network device, said system comprising:

an information request system configured to communicate with the first and second network devices,

the information request system being configured to receive an input from a user, the input corresponding to the user's intent to have encrypted information communicated to the second network device,

the information request system being further configured to receive a decryption key and information corresponding to an address from the first network device in a secure format, the information request system providing the decryption key and the information corresponding to the address to the second network device in the secure format, thereby enabling the second network device to access and retrieve encrypted information posted on the Internet at the address and decrypt the information using the decryption key,

wherein access to the address by the second network device is prevented after a predetermined period of time has elapsed, and

wherein the encrypted information is provided from the first network device to the second network device without either of the first and second network devices being identified to the other.

20. (Original) The system of claim 19, further comprising:

a mobile appliance configured to communicate with the first and second network devices; and

wherein the information request system is a part of the mobile appliance.

21. (New) The method of claim 1, wherein access for the second network device to retrieve the encrypted information is limited to a predetermined time period.

22. (New) The system of claim 12, wherein the secure tunnel system is configured to prevent the encrypted information from being retrieved by the second network device after a time limit has been reached.

23. (New) The system of claim 12, further comprising:

means for generating the first one-time use URL and the second one-time use URL.

24. (New) The method of claim 16, wherein retrieving of the encrypted information by the second network device is limited to a predetermined time period.

25. (New) The system of claim 19, wherein:

the address provided to the first network device is a first Uniform Resource Locator (URL) configured for a one-time use; and

the second network device retrieves the encrypted information using a second URL, the second URL being configured for a one-time use.